EVROPSKA
KOMISIJA

Bruselj, 9.10.2024
COM(2024) 451 final

POROČILO KOMISIJE EVROPSKEMU PARLAMENTU IN SVETU

o prvem rednem pregledu delovanja sklepa o ustreznosti glede okvira za varstvo zasebnosti podatkov med EU in ZDA

1. PRVI REDNI PREGLED – OZADJE, PRIPRAVA IN POSTOPEK

Komisija je v sklepu z dne 10. julija 2023 (v nadaljnjem besedilu: sklep o ustreznosti) ugotovila, da okvir za varstvo zasebnosti podatkov med EU in ZDA (Data Privacy Framework, v nadaljnjem besedilu: DPF EU-ZDA ali DPF) zagotavlja ustrezno raven varstva osebnih podatkov, ki se prenašajo iz Evropske unije organizacijam v Združenih državah Amerike[1]. V skladu s sklepom o ustreznosti mora Komisija izvajati redne preglede, in sicer prvega po enem letu od datuma uradnega obvestila državam članicam o sklepu o ustreznosti. To poročilo zaključuje prvi pregled.

Kot se zahteva v uvodni izjavi 211 sklepa o ustreznosti, je bil ta prvi pregled, ki je potekal po prvem letu delovanja novega okvira, osredotočen na preverjanje, ali so bili vsi elementi iz okvira izvedeni in učinkovito delujejo. Pregled je zajemal vse vidike delovanja okvira, pri čemer je bil upoštevan tudi pravni razvoj po sprejetju sklepa o ustreznosti.

Komisija je v okviru priprav na pregled pridobila informacije od ustreznih deležnikov, zlasti nevladnih organizacij s strokovnim znanjem na področju digitalnih pravic in zasebnosti[2], organizacij, certificiranih v okviru DPF, in sicer prek njihovih trgovinskih združenj[3], ter od organov ZDA, ki sodelujejo pri izvajanju okvira. Poleg tega je s posebnim pozivom k predložitvi dokazov na portalu Povejte svoje mnenje zbrala tudi povratne informacije širše javnosti[4].

Pregledovalna seja je potekala 18. in 19. julija 2024 v Washingtonu. Sejo sta odprla evropski komisar za pravosodje in potrošnike Didier Reynders in ameriška ministrica za trgovino Gina Raimondo.[5]

Na strani EU so pregled opravili predstavniki Generalnega direktorata Evropske komisije za pravosodje in potrošnike skupaj s petimi predstavniki, ki jih je imenoval Evropski odbor za varstvo podatkov (EOVP) in prihajajo iz različnih nacionalnih organov za varstvo podatkov,

---

[1] Izvedbeni sklep Komisije EU 2023/1795 z dne 10. julija 2023 v skladu z Uredbo (EU) 2016/679 Evropskega parlamenta in Sveta o ustreznem varstvu osebnih podatkov na podlagi okvira za varstvo zasebnosti podatkov med EU in ZDA.

[2] Komisija je poslala vprašalnik devetim nevladnim organizacijam (organizaciji Human Rights Watch, ameriški zvezi za državljanske svoboščine, zvezi potrošnikov Amerike, centru za digitalno demokracijo, inštitutu za odprto tehnologijo New America, organizaciji Access Now, organizaciji Electronic Frontier Foundation, informacijskemu centru za elektronsko zasebnost ter centru za demokracijo in tehnologijo), pri čemer se je osredotočila na zadevne spremembe pravnega okvira ZDA, mehanizme nadzora in izvrševanja ter delovanje mehanizmov pravnih sredstev. Službe Komisije in predstavniki Evropskega odbora za varstvo podatkov (EOVP) so se 9. julija 2024 s temi nevladnimi organizacijami sestali tudi prek spleta.

[3] Komisija je poslala vprašalnik devetim trgovinskim združenjem (združenju programske in informacijske industrije, gospodarski zbornici ZDA, industrijskemu svetu za informacijsko tehnologijo, družbi Software Alliance, centru za vodstvo informacijske politike, uradu za interaktivno oglaševanje, svetu ZDA za mednarodno poslovanje, združenju računalniške in komunikacijske industrije ter organizaciji Engine), pri čemer se je osredotočila na izkušnje podjetij, certificiranih v okviru DPF, zlasti na postopek certificiranja, ukrepe, sprejete za uskladitev z načeli DPF, mehanizme za obravnavo zahtev in pritožb posameznikov itd.

[4] Prejete povratne informacije so na voljo na naslednji povezavi: https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/14379-EU-US-Data-Privacy-Framework-report-of-the-Commission-on-how-the-framework-is-functioning_sl.

[5] Pregledovalna seja je bila organizirana po temah, pri čemer je bila vsaka namenska točka dnevnega reda uvodoma predstavljena s kratko predstavitvijo ustreznega organa ZDA, predstavnika EU ali organizacije, temu pa je sledila podrobna razprava z vprašanji in odgovori. Prvi dan so bili obravnavani „trgovinski vidiki“ okvira (tj. uporaba in izvrševanje zahtev, ki se uporabljajo za družbe, certificirane v okviru z DPF), drugi dan pa vprašanja v zvezi z vladnim dostopom do osebnih podatkov.

ter Evropskim nadzornikom za varstvo podatkov[6]. ZDA so zastopali predstavniki ministrstva za trgovino, ministrstva za zunanje zadeve, zvezne komisije za trgovino (Federal Trade Commission, v nadaljnjem besedilu: FTC), ministrstva za promet, urada direktorja nacionalne obveščevalne službe (Office of the Director of National Intelligence, v nadaljnjem besedilu: ODNI), ministrstva za pravosodje, generalnega inšpektorja obveščevalne skupnosti ter člani nadzornega odbora za zasebnost in državljanske svoboščine (Privacy and Civil Liberties Oversight Board, v nadaljnjem besedilu: PCLOB). Poleg tega so na ustreznih pregledovalnih sejah informacije zagotovili predstavniki organizacij, ki nudijo neodvisne storitve reševanja sporov, in ameriškega združenja za arbitražo. Pregled je vključeval tudi predstavitve organizacij, certificiranih v okviru DPF, o tem, kako družbe izpolnjujejo zahteve okvira.

Ugotovitve Komisije so bile nadalje podprte z javno dostopnim gradivom, kot so sodne odločbe, izvedbena pravila in postopki ustreznih organov ZDA, poročila in študije nevladnih organizacij, poročila o preglednosti, ki so jih izdale družbe, certificirane v okviru DPF, letna poročila neodvisnih nadzornih organov in poročila medijev.

2. UGOTOVITVE

2.1. Trgovinski vidiki

2.1.1. Postopek certificiranja

Da bi družba iz ZDA lahko prejemala osebne podatke, prenesene iz EU na podlagi DPF, mora pri ministrstvu za trgovino certificirati in nato vsako leto ponovno certificirati zavezanost posebnim zahtevam glede varstva podatkov (v nadaljnjem besedilu: načela DPF). Za certificiranje morajo za družbo veljati preiskovalna in izvršilna pooblastila FTC ali ministrstva za promet, družba mora javno razglasiti svojo zavezanost načelom DPF ter javno razkriti svojo politiko zasebnosti in take zahteve v celoti izvajati[7]. Ministrstvo za trgovino pred zaključkom certificiranja preveri, ali je družba izpolnila vse zahteve za certificiranje[8].

Ministrstvo za trgovino je na pregledovalni seji pojasnilo, da je bil v prvem letu DPF poudarek na vzpostavitvi postopka certificiranja, vključno z razvojem posebnih orodij IT, posodobitvi postopkov, sodelovanju z družbami in izvajanju drugih dejavnosti ozaveščanja. Na dan pregledovalne seje je bilo v okviru DPF certificiranih več kot 2 800 družb. To pomeni, da je bilo v okviru DPF certificiranih več družb kot v prvem letu delovanja prejšnjega okvira, tj. zasebnostnega ščita[9]. Glede na informacije, ki jih je predložilo ministrstvo za trgovino, je 70 % udeležencev MSP, veliko družb, ki so se pridružile DPF (47 %), pa je iz sektorja informacijske in komunikacijske tehnologije (IKT). Poleg tega je 60 % družb certificiranih izključno za podatke, ki niso o človeških virih, 2,5 % za podatke o človeških virih, 37,5 % pa za podatke o človeških virih in podatke, ki niso o človeških virih.

Ministrstvo za trgovino je sprejelo potrebne postopke za obravnavo vlog družb. Družbe morajo svoje vloge za certificiranje predložiti na spletišču ministrstva za trgovino o DPF

[6] Predstavniki Komisije in EOVP so se sestali 12. junija in 10. julija 2024, da bi se pripravili na pregled, razpravljali o prejetih prispevkih in opredelili, glede katerih vidikov je treba zbrati dodatne informacije in pojasnila.
[7] Oddelek I.2 Priloge I k sklepu o ustreznosti.
[8] Priloga III k sklepu o ustreznosti.
[9] V enakem obdobju je certifikat v okviru zasebnostnega ščita pridobilo 2 400 družb.

(https://www.dataprivacyframework.gov/). To spletišče vsebuje informacije o tem, kako se pridružiti DPF[10], in o obveznostih družb v skladu z navedenim okvirom[11]. Posebna skupina v okviru ministrstva za trgovino, za katero je odgovoren poseben direktor za okvir za varstvo zasebnosti podatkov, je odgovorna za vse vidike, povezane z upravljanjem in vodenjem DPF, vključno s postopkom certificiranja in spremljanjem skladnosti. Posamezna vloga se dodeli določenemu članu osebja, ki je odgovoren za zadevno družbo med celotnim postopkom certificiranja.

Da bi bile certificirane v skladu z okvirjem, morajo družbe predložiti vlogo, vključno z osnutkom politike zasebnosti. Ministrstvo za trgovino preveri, ali družba izpolnjuje ustrezne zahteve DPF. Kadar želijo organizacije certificirati različne subjekte v skupini podjetij (npr. različne podružnice), ministrstvo za trgovino zahteva in pregleda bodisi eno celovito politiko zasebnosti, v kateri so jasno navedeni vsi subjekti, ki jih je treba zajeti, bodisi ločene politike za vsak subjekt. Ministrstvo za trgovino z neodvisnim pritožbenim mehanizmom[12], navedenim v vlogi, preverja tudi, ali se je organizacija pri njem dejansko registrirala. Če družba izbere forum organov za varstvo podatkov (npr. ker obdeluje podatke o človeških virih), ministrstvo za trgovino preveri, ali je plačala zahtevano pristojbino za uporabo foruma. Ministrstvo za trgovino po potrebi preveri tudi, ali prosilec spada v pristojnost FTC ali ministrstva za promet (in se ima zato pravico pridružiti DPF).

Če so izpolnjeni vsi pogoji, ministrstvo za trgovino obvesti organizacijo, da lahko na svojem spletišču objavi politiko zasebnosti, ki se sklicuje na DPF. Ko je politika zasebnosti javna, ministrstvo za trgovino potrdi certificiranje in družbo vključi na seznam DPF na svojem spletišču. DPF je mogoče uporabiti za prejemanje osebnih podatkov iz EU od datuma, ko ministrstvo za trgovino uvrsti organizacijo na navedeni seznam[13].

Kot je bilo pojasnjeno na pregledovalni seji, je bilo na podlagi pregledov, ki jih je ministrstvo za trgovino izvedlo do zdaj, zavrnjenih 33 vlog, ker niso izpolnjevale zahtev DPF. Na splošno ministrstvo za trgovino sodeluje z družbo pri odpravljanju morebitnih pomanjkljivosti. Kadar ministrstvo za trgovino ugotovi kakršne koli pomanjkljivosti, obvesti družbo, da jih mora odpraviti in da se bo štelo, da je odstopila od obravnavane vloge, če se ne bo odzvala v določenem roku ali če ne bo opravila svojega samocertificiranja v skladu s postopki ministrstva za trgovino. Če se začetno certificiranje ne opravi/spremeni v 12 mesecih, ministrstvo za trgovino šteje, da je družba od vloge odstopila.

Rok za letno ponovno certificiranje je za vsako družbo določen na seznamu DPF. Za opozarjanje družb, da morajo vložiti vlogo za ponovno certificiranje, je ministrstvo za trgovino vzpostavilo sistem z opomniki o skorajšnjem poteku certificiranja. Organizacije prejmejo opomnik en mesec pred rokom, nato dva tedna pred rokom in nato še en dan pred rokom. Organizacije, katerih certificiranje poteče, se odstranijo s seznama DPF. Kot je opisano v Prilogi III k sklepu o ustreznosti, ima ministrstvo za trgovino na svojem spletišču poseben oddelek, v katerem so navedeni organizacije iz ZDA, ki niso več dejavne udeleženke, in ustrezni razlogi, zakaj so bile zadevne družbe (npr. potek ali izstop) odstranjene s seznama (v nadaljnjem besedilu: seznam neaktivnih organizacij). Če so organizacije odstranjene s seznama

[10] https://www.dataprivacyframework.gov/program-articles/How-to-Join-the-Data-Privacy-Framework-(DPF)-Program-(part%E2%80%931).

[11] https://www.dataprivacyframework.gov/key-requirements.

[12] Mehanizmi za reševanje sporov v zasebnem sektorju, s katerimi se pritožbe in spori vsakega posameznika preiščejo in hitro razrešijo brez stroška za posameznika.

[13] Oddelek I, odstavek 3, Priloge I k sklepu o ustreznosti.

DPF, ker so pustile, da njihovo certificiranje poteče, ministrstvo za trgovino stopi v stik z njimi, da potrdijo, ali želijo izstopiti ali se namesto tega ponovno certificirati, in v slednjem primeru preveri, ali so od poteka uporabljale načela DPF za osebne podatke, ki so jih prejele v okviru DPF, ter da pojasnijo, katere ukrepe bodo sprejele za obravnavanje nerešenih težav, zaradi katerih je prišlo do zamude pri ponovnem certificiranju. Če družbe obvestijo ministrstvo za trgovino, da želijo izstopiti iz DPF, ministrstvo za trgovino od njih zahteva, da potrdijo, ali bodo podatke, prejete v okviru DPF, vrnile ali izbrisale, jih hranile in še naprej uporabljale načela DPF za take podatke (kar je treba potrditi vsako leto), ali jih hranile in vzpostavile drugo zaščito (kot so standardne pogodbene klavzule, ki jih je sprejela Evropska komisija).

Povratne informacije, prejete od trgovinskih združenj in družb, kažejo, da so družbe, certificirane v okviru DPF, sprejele številne ukrepe za zagotovitev skladnosti z načeli DPF. Na primer, za izpolnjevanje *načela pritožbenega mehanizma, izvrševanja in odgovornosti* so organizacije izvedle notranje preglede, bodisi s samoocenjevanjem bodisi z zunanjim pregledom skladnosti. Dva neodvisna pritožbena mehanizma zasebnega sektorja, ki sta sodelovala na pregledovalni seji, sta pojasnila, da s pregledovanjem politik zasebnosti zagotavljata tudi zunanji pregled skladnosti, eden od njiju pa je pojasnil, da zagotavlja tudi revizije in naključne preglede, pri čemer se na primer osredotoča na načela *dostopa*, *izbire* in *nadaljnjega prenosa*. Poleg tega so certificirane družbe razvile notranje programe skladnosti in nadzorne mehanizme, usposobile zaposlene, uvedle mehanizme, ki posameznikom omogočajo uveljavljanje njihovih pravic, izvedle ocene učinka na varstvo zasebnosti in pregledale obstoječe pogodbe.

2.1.2. Spremljanje skladnosti, lažne navedbe o sodelovanju in izvrševanje

Ministrstvo za trgovino je v skladu z DPF odgovorno za spremljanje skladnosti z načeli DPF z uporabo različnih orodij, vključno s pregledi po uradni dolžnosti (na lastno pobudo), *ad hoc* pregledi na kraju samem in vprašalniki o skladnosti. To vključuje iskanje in obravnavanje lažnih navedb o sodelovanju v okviru, na primer s spletnimi iskanji[14].

Ministrstvo za trgovino se je pri spremljanju skladnosti družb v DPF z načeli v preteklem letu zanašalo predvsem na *ad hoc* spletna iskanja in preglede (družbenih) medijev. Ministrstvo za trgovino je poročalo, da v tem prvem letu ni odkrilo težav v zvezi s skladnostjo z načeli DPF in da v zvezi z nobeno družbo ni odstopilo zadeve FTC ali ministrstvu za promet za morebitno uvedbo pregona. Imenovalo je tudi posebno osebo za stike, da bi olajšala sodelovanje z organi za varstvo podatkov ter sprejemala pritožbe posameznikov in predložene zadeve drugih organov (npr. organov za varstvo podatkov ali FTC). Vendar v preteklem letu ni bila prejeta nobena predložena zadeva ali pritožba. Medtem ko je bil DPF prvo leto delovanja osredotočen na vzpostavitev okvira in postopka certificiranja, je ministrstvo za trgovino na pregledovalni seji pojasnilo, da namerava izvajati preverjanja skladnosti z avtomatiziranimi sredstvi, da bi se izvajala bolj sistematično, in trenutno razvija orodja IT, ki so za to potrebna.

Komisija priznava, da je moralo ministrstvo za trgovino svoja prizadevanja v tem prvem letu osredotočiti na vzpostavitev okvira in postopek certificiranja. V prihodnje je pomembno, da ministrstvo za trgovino okrepi svoja prizadevanja za spremljanje in preverjanje skladnosti z načeli, kar je nujno za zagotavljanje stalne visoke ravni skladnosti z okvirom in odkrivanje primerov, za katere so potrebni nadaljnji izvršilni ukrepi, vključno z morebitnimi lažnimi

[14] Glej Prilogo III k sklepu o ustreznosti. Lažne navedbe se lahko na primer pojavijo, kadar družba trdi, da sodeluje v DPF, in ni nikoli začela postopka certificiranja ali pa ga je začela, vendar ga ni končala, ali je dopustila, da je certificiranje poteklo.

navedbami družb o sodelovanju. V zvezi s tem Komisija pozdravlja dejstvo, da je ministrstvo za trgovino potrdilo, da namerava razviti in uporabljati (avtomatizirana) orodja za učinkovitejše in bolj sistematično odkrivanje težav v zvezi s skladnostjo in lažnih navedb, ter meni, da bi to moralo biti del širših prizadevanj za večjo uporabo različnih orodij, ki jih ima na voljo (npr. pregledi na kraju samem, vprašalniki za pregled skladnosti, zahteve po informacijah itd.), vključno s preverjanjem skladnosti s posebnimi zahtevami iz DPF[15].

Organizacije v DPF so v pristojnosti FTC in ministrstva za promet. Ministrstvo za promet je na pregledovalni seji potrdilo, da ima vzpostavljene vse postopke za uvedbo ustreznega kazenskega pregona. Pojasnilo je tudi, da se je DPF pridružilo zelo malo družb, ki so v njegovi pristojnosti (tj. nekaj agencij za prodajo letalskih vozovnic, vendar noben letalski prevoznik). FTC je potrdil, da v vsaki preiskavi varovanja zasebnosti sistematično preverja kršitve DPF. Do zdaj mu drugi organi niso predložili nobene zadeve. Prejel je nekaj pritožb, v katerih je bil omenjen DPF, vendar sta se dve nanašali na družbi na seznamu neaktivnih organizacij, dve na družbi, ki nista sodelovali v okviru, ena pa se ni nanašala na osebne podatke, prenesene iz EU. FTC do tega poročila ni izdal sklepov za uveljavljanje skladnosti z DPF, čeprav je potrdil, da trenutno preiskuje več družb, certificiranih v okviru DPF.

Komisija pozdravlja dejstvo, da FTC sistematično preverja kršitve DPF v vseh svojih preiskavah varovanja zasebnosti. Ker je nadaljnja učinkovitost DPF odvisna od njegovega doslednega izvrševanja, se pričakuje, da bo FTC še naprej izvajal svoja preiskovalna pooblastila v skladu z okvirom, vključno z dejavnim izvajanjem usmerjenih preiskav, osredotočenih na skladnost s posebnimi zahtevami DPF in/ali nekatere sektorje.

2.1.3. Reševanje pritožb

DPF posameznikom iz EU zagotavlja različne možnosti pritožbenih mehanizmov, kadar certificirane organizacije ne spoštujejo načel DPF[16]. To vključuje reševanje z neposrednimi stiki z organizacijo v DPF, ki mora zadevnemu posamezniku odgovoriti v 45 dneh. Posamezniki lahko pritožbo vložijo tudi pri neodvisnem pritožbenem mehanizmu, ki ga organizacija imenuje za preiskovanje in reševanje pritožb. To je lahko organ za alternativno reševanje sporov ali organ za varstvo podatkov[17], odvisno od okoliščin. Nazadnje, če se pritožba posameznika, na katerega se nanašajo osebni podatki, ne reši zadovoljivo z uporabo katere izmed navedenih možnosti pravnega varstva, lahko posamezniki v skrajnem primeru sprožijo zavezujočo arbitražo pred senatom DPF EU-ZDA.

2.1.3.1. Obravnava pritožb s strani družb

Odgovori trgovinskih združenj in družb na vprašalnike, ki jih je poslala Komisija, kažejo, da so družbe, certificirane v okviru DPF, prejele zelo malo pritožb posameznikov v zvezi z neskladnostjo z načeli DPF ali sploh nobene. Hkrati so družbe vzpostavile različne mehanizme in orodja, ki posameznikom omogočajo uveljavljanje njihovih pravic in vlaganje pritožb, tudi prek spletnih obrazcev, elektronske pošte in telefona.

2.1.3.2. *Neodvisni pritožbeni mehanizmi*

[15] Na primer v zvezi z nadaljnjimi prenosi z uporabo možnosti iz načela DPF 3(b), da se zahteva povzetek ali reprezentativni izvod ustreznih določb o zasebnosti iz pogodb o nadaljnjih prenosih.
[16] Glej oddelek 2.4 sklepa o ustreznosti.
[17] Organizacije v DPF morajo sodelovati pri preiskavi in reševanju pritožbe organa za varstvo podatkov, če se nanaša na obdelavo podatkov o človeških virih, zbranih v okviru delovnega razmerja, ali če so prostovoljno sprejele nadzor organov za varstvo podatkov.

Povratne informacije, prejete na pregledovalni seji, in informacije, ki so jih predložila trgovinska združenja, kažejo, da je bilo pri neodvisnih pritožbenih mehanizmih vloženih zelo malo pritožb. Neodvisni pritožbeni mehanizmi, ki so jih izbrale družbe, vključujejo BBB National Programs, JAMS, TRUSTe in VeraSafe. V skladu z DPF morajo neodvisni pritožbeni mehanizmi objaviti letno poročilo z zbirnimi statističnimi podatki o uporabi njihovih storitev za reševanje sporov. Do sprejetja tega poročila so vsi zadevni neodvisni pritožbeni mehanizmi objavili svoja letna poročila[18].

Poleg tega sta družbi BBB in VeraSafe na pregledovalni seji podrobno predstavili svoje dejavnosti v preteklem letu. Poročali sta, da je v primerjavi s prejšnjimi okviri njune storitve izbralo več poslovnih udeležencev, in navedli, da sta prejeli nekaj pritožb, od katerih velika večina ni bila upravičena. Družba BBB je na primer prejela 87 pritožb posameznikov iz EU, od katerih sta bili le dve upravičeni do reševanja. Čeprav je družba BBB pojasnila, da se pritožbe v povprečju obravnavajo v petih delovnih dneh, sta bili ti pritožbi nazadnje zaključeni, ker se posameznika nista odzvala. Družba VeraSafe je prejela 26 pritožb, od katerih jih je bilo šest upravičenih do reševanja. Dve, ki sta se nanašali na zahtevi za dostop in izbris, sta bili rešeni, dve sta še v obravnavi, dve pa sta bili umaknjeni ali zaključeni, ker se posameznik ni odzval. Oba neodvisna pritožbena mehanizma sta pojasnila, da nameravata na pritožbe odgovoriti v jeziku posameznika.

Družbe v DPF, ki obdelujejo podatke o človeških virih, prenesene iz EU, morajo izbrati organe EU za varstvo podatkov kot svoj neodvisni pritožbeni mehanizem za te podatke, medtem ko lahko za druge vrste osebnih podatkov, prenesenih na podlagi DPF, organe EU za varstvo podatkov kot svoj neodvisni pritožbeni mehanizem izberejo prostovoljno. Za to rešitev[19] se je odločila več kot polovica družb, certificiranih v okviru DPF med pregledom, kar je dobrodošlo. EOVP je od sprejetja sklepa o ustreznosti sprejel poslovnik „neuradnega foruma organov za varstvo podatkov EU“. Forum je pristojen za zagotavljanje zavezujočih nasvetov organizacijam ZDA po nerešenih pritožbah posameznikov v okviru DPF glede ravnanja z osebnimi podatki, ki so bili preneseni iz EU v skladu z DPF. Forum v skladu s poslovnikom sestavljajo organ za varstvo podatkov, ki deluje kot vodilni organ za varstvo podatkov, in drugi organi za varstvo podatkov, imenovani kot sopregledovalci[20]. Forum v 60 dneh po prejemu

[18] ANA – https://www.ana.net/content/show/id/accountability-dpf-consumers;
BBB National Programs – https://assets.bbbprograms.org/docs/default-source/eu-privacy-shield/dpf_periodicalreport_072024.pdf; ICDR – AAA – https://go.adr.org/rs/294-SFS-516/images/Data%20Privacy%20Framework%20IRM%20Program%20Report%202023-2024%20FINAL.pdf?version=0;
združenje Insights – https://www.insightsassociation.org/Portals/INSIGHTS/Insights%20Association%20DPF%20Services%20Program%202024%20Annual%20Report_Final_1.pdf;
JAMS – https://www.jamsadr.com/files/Uploads/Documents/2024-Annual-Report-DPF-Cases.pdf;
Privacy Trust DPF Services – https://privacytrust.com/fserve/PrivacyTrust_Dispute_Resolution_Report_2023_2024.pdf;
TRUSTe Dispute Resolution – https://trustarc.com/wp-content/uploads/2024/07/2024-Independent-Recourse-Mechanism-Annual-Report.pdf;
Verasafe – https://verasafe.com/wp-content/uploads/2020/06/VeraSafe-DPF-Dispute-Resolution-Program-Annual-Report-2024.pdf.

[19] Kmalu po datumu pregledovalne seje je bilo na spletišču o DPF navedeno, da je 1 511 od 2 892 udeležencev za pritožbeni mehanizem izbralo organ EU za varstvo podatkov.

[20] EOVP je 17. aprila 2024 sprejel poslovnik „neuradnega foruma organov za varstvo podatkov EU“ v skladu z okvirom za varstvo zasebnosti podatkov med EU in ZDA. Na voljo je na naslednjem naslovu: https://www.edpb.europa.eu/system/files/2024-04/dpf_rules-of-procedure_informal-panel-dpas_en.pdf.

pritožbe v okviru DPF zagotovi zavezujoče nasvete. EOVP je objavil tudi predlogo obrazca za vložitev pritožb pri organih za varstvo podatkov[21] ter pogosto zastavljena vprašanja glede DPF za evropske posameznike[22] in družbe[23]. Forum med pregledom ni prejel nobene pritožbe.

2.1.3.3. Mehanizem zavezujoče arbitraže

Ministrstvo za trgovino je za upravljanje mehanizma zavezujoče arbitraže izbralo mednarodno središče za reševanje sporov (International Centre for Dispute Resolution, v nadaljnjem besedilu: ICDR), ki je mednarodni oddelek ameriškega združenja za arbitražo. Ministrstvo za trgovino je po sprejetju sklepa o ustreznosti skupaj s Komisijo izbralo enajst arbitrov z različnih področij, vključno z arbitražo, sodstvom, akademskimi krogi in civilno družbo, z izkušnjami na področju varstva zasebnosti[24]. Poleg tega so bila sprejeta arbitražna pravila[25] za senat DPF in kodeks ravnanja za arbitre[26], ki so na voljo na spletišču ICDR. Ob pregledu noben posameznik iz EU še ni sprožil mehanizma arbitraže.

2.1.4. Smernice, sodelovanje in ozaveščanje

Ministrstvo za trgovino je od začetka veljavnosti DPF izvajalo različne dejavnosti ozaveščanja, tako da je organiziralo potujoče kampanje, spletne seminarje in konference, vzpostavljalo stike s trgovinskimi združenji in neposredno sodelovalo z več kot 3 000 družbami, da bi jim zagotovilo informacije o DPF. Objavilo je tudi smernice, med drugim v obliki pogosto zastavljenih vprašanj, naslovljenih na posameznike, ter družbe v EU in ZDA[27]. EOVP je nato pripravil obrazce za pritožbe in pogosto zastavljena vprašanja, naslovljena na posameznike in družbe. Podobno je Komisija ob sprejetju sklepa o ustreznosti objavila vprašanja in odgovore ter informativni pregled o DPF[28].

Hkrati se je na pregledovalni seji izkazalo, da si je treba bolj prizadevati za ozaveščanje posameznikov in zagotavljanje smernic družbam. Podatki, ki so jih zagotovile družbe in neodvisni pritožbeni mehanizmi, ter zelo majhno število pritožb kažejo, da posamezniki morda niso vedno seznanjeni s svojimi pravicami in/ali mehanizmom za njihovo uveljavljanje. Ministrstvo za trgovino je na pregledovalni seji izrazilo zanimanje za sodelovanje z organi za varstvo podatkov EU, da bi povečali ozaveščenost posameznikov iz EU o okviru. Komisija spodbuja take pobude in tudi sprejema ukrepe za boljše obveščanje posameznikov, med drugim tako, da na svojem spletišču zagotavlja dodatne informacije o DPF, na primer z vključitvijo povezav in sklicev na ustrezne smernice, ki so jih sprejeli EOVP, ministrstvo za trgovino in drugi organi ZDA.

Glede smernic o načelih DPF so se predstavniki EOVP na pregledovalni seji dogovorili, da bodo v prihodnjih mesecih sodelovali, da bi zagotovili dodatna pojasnila o pojmu podatkov o

[21] https://www.edpb.europa.eu/our-work-tools/our-documents/other-guidance/eu-us-data-privacy-framework-template-complaint-form_sl.
[22] https://www.edpb.europa.eu/our-work-tools/our-documents/other-guidance/eu-us-data-privacy-framework-faq-european-individuals_sl.
[23] https://www.edpb.europa.eu/our-work-tools/our-documents/other-guidance/eu-us-data-privacy-framework-faq-european-businesses_sl.
[24] https://go.adr.org/DPF_Arbitrator_Bios.html.
[25] https://go.adr.org/rs/294-SFS-516/images/IC.DR-AAA_EU-US_DPF_AnnexI_Arbitration_Rules.pdf.
[26] https://go.adr.org/rs/294-SFS-516/images/Code_of_Conduct_for_Arbitrators_Appointed_to_EU-US_DPF_AnnexI_Arbitrations.pdf.
[27] Glej npr. https://www.dataprivacyframework.gov/US-Businesses.
[28] https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/eu-us-data-transfers_sl.

človeških virih v skladu z DPF in posebnih obveznostih v zvezi z obdelavo takih podatkov. Preučeni so bili različni elementi, ki jih je treba vključiti v take smernice. V teh smernicah bi se lahko na primer obravnavali nekateri praktični scenariji, v katerih bi se podatki o zaposlenih obdelovali v skladu z DPF (npr. s strani ponudnika storitev v oblaku), in pojasnilo, katere obveznosti iz DPF bi bile v teh scenarijih ustrezne. Poleg tega bi lahko družbam, ki prejemajo podatke o zaposlenih posameznikov iz EU (vendar takih podatkov ne uporabljajo nujno v okviru delovnega razmerja), predlagale, naj za svoj neodvisni pritožbeni mehanizem izberejo forum organov za varstvo podatkov. S tem bi se zagotovilo, da se lahko ti posamezniki obrnejo na organ, ki je „v bližini doma“ in je po potrebi bolje seznanjen z veljavno nacionalno zakonodajo, ki se uporablja za podatke o človeških virih.

Poleg tega se poseben vidik nanaša na zahteve DPF za nadaljnje prenose, za katere bi bilo smiselno zagotoviti več smernic (tudi na podlagi podatkov trgovinskih združenj). Ministrstvo za trgovino je tudi navedlo, da bi bilo vredno preučiti, ali bi nekaterim sektorjem koristile dodatne smernice o uporabi načel DPF pri njihovih dejavnostih, npr. na področju zdravstvenih raziskav in finančnih storitev.

Komisija pozdravlja pripravljenost obeh strani, da pripravita smernice, in pričakuje, da se bo delo v zvezi z zgoraj navedenimi temami kmalu začelo.

Na splošno je bilo vzpostavljenih več mehanizmov za zagotavljanje izmenjav in sodelovanja med organi ZDA in organi za varstvo podatkov, vključno z imenovanjem posebnih oseb za stike v okviru FTC in ministrstva za trgovino za obravnavo poizvedb in zadev, ki bi jih predložili organi za varstvo podatkov.

2.1.5. Razvoj dogodkov v zvezi s pravnim sistemom ZDA

Od sprejetja sklepa o ustreznosti je prišlo do številnih sprememb v pravnem okviru ZDA na področju zasebnosti. To vključuje razvoj zakonodaje, predpisov in sodne prakse. Spremembe na splošno kažejo na okrepljeno zbliževanje pristopov EU in ZDA k nekaterim izzivom v zvezi z zasebnostjo, tudi z uporabo podobnih pravnih pojmov. Nekatere od njih še potekajo in jih bo treba še naprej spremljati.

Na zvezni ravni je predsednik izdal več odredb, ki so pomembne za uporabo osebnih podatkov. Zlasti Odredba št. 14117 z dne 28. februarja 2024[29] prepoveduje ali omejuje transakcije, ki vključujejo nekatere kategorije občutljivih osebnih podatkov (npr. zdravstvene podatke, biometrične identifikatorje, človeške genomske podatke), s subjekti v nekaterih „zadevnih državah“[30]. S sprejeto odredbo se generalnemu državnemu tožilcu nalaga, naj predlaga predpise, ki ob sprejetju tega poročila še niso bili izdani, da se podrobneje opredeli njeno izvajanje. Poleg tega je Odredba št. 14110 z dne 30. oktobra 2023 o umetni inteligenci[31] osredotočena na razvoj varne, zanesljive in zaupanja vredne umetne inteligence. Od več zveznih agencij zahteva, da razvijejo varnostne standarde in smernice, povezane z umetno

[29] https://www.federalregister.gov/documents/2024/03/01/2024-04573/preventing-access-to-americans-bulk-sensitive-personal-data-and-united-states-government-related.

[30] Te vključujejo Kitajsko, Kubo, Hongkong in Macau, Iran, Severno Korejo ter Venezuelo, kot je predlagal generalni državni tožilec v predhodnem obvestilu o predlaganem oblikovanju predpisov z dne 3. maja 2024. Glej https://www.federalregister.gov/documents/2024/03/05/2024-04594/national-security-division-provisions-regarding-access-to-americans-bulk-sensitive-personal-data-and.

[31] https://www.federalregister.gov/documents/2023/11/01/2023-24283/safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence.

inteligenco, tudi o posebnih tveganjih umetne inteligence za zasebnost in tehnikah za ohranjanje zasebnosti.

Kar zadeva zakonodajno delo, je v zadnjih letih kongres uvedel zvezne predloge zakona o zasebnosti, 20 ameriških zveznih držav pa je do julija 2024 sprejelo celovite zakone o zasebnosti, od katerih se jih je osem začelo uporabljati: v Kaliforniji, Koloradu, Oregonu, Virginiji, Connecticutu, Utahu, Teksasu in na Floridi. Poleg tega je 17 ameriških zveznih držav sprejelo zakonodajo, ki obravnava avtomatizirano obdelavo (ali vsaj nekatere njene oblike) in na splošno dovoljuje zavrnitev nekaterih vrst odločanja na podlagi „oblikovanja profilov“[32].

Kar zadeva razvoj sodne prakse, je več predstavnikov civilne družbe opozorilo na nedavno sodbo vrhovnega sodišča v zadevi Loper Bright Enterprises proti Raimondo (z dne 28. junija 2024). Ta sodba razveljavlja prejšnjo sodno prakso o doktrini Chevron, v skladu s katero sodišča v primeru dvoumnosti v zakonu, ki ga izvršuje regulativna agencija, uporabijo načelo upoštevanja razumne razlage prava, ki jo poda ta agencija. Nekatere nevladne organizacije so zlasti izrazile pomisleke glede vpliva te sodbe vrhovnega sodišča na pristojnost FTC za oblikovanje predpisov na področju zasebnosti, hkrati pa so priznale, da morda nima vpliva na izvršilna pooblastila FTC ali pa je ta omejen. FTC je na pregledovalni seji sporočil, da je še prezgodaj, da bi vedeli, kakšne točno bodo posledice te sodbe. Hkrati je pojasnil, da se oblikovanje predpisov FTC izvaja v skladu s pooblastilom iz zakona o FTC, ki se razlikuje od pooblastil drugih upravnih agencij in za katere je doktrina Chevron manj pomembna. Zato je vpliv nedavne sodbe na tem področju morda omejen.

Poleg tega je FTC sporočil nedavne spremembe svojega pristopa k avtomatizirani obdelavi in umetni inteligenci. To vključuje sprejetje skupne izjave skupaj z drugimi izvršilnimi organi proti diskriminaciji in pristranskosti v avtomatiziranih sistemih[33] ter več izvršilnih ukrepov, pri katerih se FTC med drugim osredotoča na preglednost in pravičnost avtomatizirane obdelave ter zmožnost posameznikov, da izpodbijajo rezultate. Najvidnejši primer v zvezi s tem je sklep FTC proti Rite Aid marca 2024, s katerim je bila tej družbi iz varnostnih razlogov naložena petletna prepoved uporabe tehnologije za prepoznavanje obrazov[34]. FTC je zlasti ugotovil, da družba Rite Aid ni sprejela razumnih ukrepov za preprečevanje napačnih rezultatov in obveščanje potrošnikov o uporabljeni tehnologiji. Na splošno je FTC na pregledovalni seji

[32] Čeprav se pomen „oblikovanja profilov“ med zveznimi državami razlikuje, je oblikovanje profilov na splošno opredeljeno kot vsaka oblika avtomatizirane obdelave osebnih podatkov za ocenjevanje, analizo ali predvidevanje osebnih vidikov, povezanih z ekonomskim položajem, zdravjem, osebnim okusom, interesi, zanesljivostjo, vedenjem, lokacijo ali gibanjem določenega ali določljivega posameznika. Običajno so potrošniki tisti, ki se lahko odločijo za zavrnitev oblikovanja profilov. Zakonodajo o oblikovanju profilov so razvile naslednje zvezne države: Kolorado (revidirani zakon Kolorada s komentarjem, člen 6-1-1306), Connecticut (splošni zakon Connecticuta s komentarjem, člen 42-518), Delaware (zakonik Delawara s komentarjem, naslov 6, člen 12D-104), Florida (zakon Floride s komentarjem, člen 501.705), Indiana (zakonik Indiane s komentarjem, člen 24-15-3-1), Kentucky (revidirani zakon Kentuckyja s komentarjem, člen 367.3615), Maryland (zakon o zasebnosti na spletu zvezne države Maryland iz leta 2024, sprejet 9. maja 2024), Minnesota (zakon Minnesote s komentarjem, člen 325O.07), Montana (zakonik Montane s komentarjem, člen 30-14-2808), Nebraska (revidirani zakon Nebraske s komentarjem, člen 87-1107), New Hampshire (revidirani zakon New Hampshira s komentarjem, člen 507-H:4), New Jersey (zakon New Jerseyja s komentarjem, člen 56:8-166.8), Oregon (revidirani zakon Oregona s komentarjem, člen 646A.574), Rhode Island (zakon o preglednosti podatkov in varstvu zasebnosti zvezne države Rhode Island, sprejet 29. junija 2024), Tennessee (zakonik Tennesseeja s komentarjem, člen 47-18-3304), Teksas (poslovni in trgovinski zakonik Teksasa s komentarjem, člen 541.051) in Virginija (zakonik Virginije s komentarjem člen 59.1-577).

[33] https://files.consumerfinance.gov/f/documents/cfpb_joint-statement-enforcement-against-discrimination-bias-automated-systems_2023-04.pdf.

[34] https://www.ftc.gov/legal-library/browse/cases-proceedings/2023190-rite-aid-corporation-ftc-v.

obravnaval svoje trenutne prednostne naloge in predvsem področja, za katera meni, da si v prihodnje zaslužijo bolj proaktiven pristop k izvrševanju. To vključuje varstvo občutljivih podatkov (npr. zdravstvenih podatkov, biometričnih podatkov, geolokacije)[35], varstvo otrok[36] in mladoletnikov na spletu ter varnost podatkov[37].

Komisija bo še naprej pozorno spremljala te in druge dogodke v ZDA, zlasti vse nadaljnje korake v smeri celovitega zveznega zakona o zasebnosti, in morebiten vpliv nedavne sodne prakse vrhovnega sodišča na vlogo FTC na področju zasebnosti.

Komisija pozdravlja informacije, ki jih je FTC zagotovil o svojih nedavnih dejavnostih izvrševanja in trenutnih prednostnih nalogah, ki v veliki meri ustrezajo trendom in prednostnim nalogam pri izvrševanju varstva podatkov v Evropi. FTC dejavno sodeluje tudi v mreži držav, ki prejemajo ugodnosti iz sklepa EU o ustreznosti, ki ga je Komisija začela izvajati marca 2024[38]. To okrepljeno zbliževanje bi moralo spodbuditi in olajšati tesnejše sodelovanje med organi za uveljavljanje varstva zasebnosti na obeh straneh Atlantika, zlasti pri zadevah, ki so pomembne za delovanje DPF.

2.2. Vidiki, povezani z dostopom do osebnih podatkov, ki jih javni organi v ZDA prenesejo v skladu z okvirom za varstvo zasebnosti podatkov med EU in ZDA, in uporaba teh podatkov

Sklep o ustreznosti vsebuje podrobno oceno pravil, ki urejajo zbiranje in uporabo osebnih podatkov, ki jih javni organi v ZDA prenesejo iz EU družbam, certificiranim v okviru DPF, zlasti za namene preprečevanja, odkrivanja in preiskovanja kaznivih dejanj ter nacionalne varnosti. Organi ZDA so na pregledovalni seji potrdili, da od sprejetja sklepa o ustreznosti v prvem letu delovanja DPF ni bilo pomembnega razvoja v zvezi s pravnim okvirom, ki se uporablja za dostop do podatkov za namene preprečevanja, odkrivanja in preiskovanja kaznivih dejanj ali regulativne namene. Zato se spodnje ugotovitve nanašajo le na razvoj na področju nacionalne varnosti.

Ugotovitve iz sklepa o ustreznosti glede dostopa obveščevalnih agencij do podatkov temeljijo na analizi pogojev in omejitev, ki se uporabljajo za obveščevalne dejavnosti SIGINT na podlagi več ustreznih pravnih pooblastil, zlasti člena 702 zakona o nadzoru tujih obveščevalnih podatkov (Foreign Intelligence Surveillance Act, v nadaljnjem besedilu: FISA) in Odredbe št. 12333[39] – kot je bila dopolnjena in okrepljena z Odredbo št. 14086 o krepitvi zaščitnih

---

[35] Glej npr. nedavno odločbo FTC zoper družbo X-Mode zaradi prodaje in izmenjave občutljivih informacij o lokaciji (https://www.ftc.gov/system/files/ftc_gov/pdf/X-ModeSocialDecisionandOrder.pdf) in zoper družbo Monument v zvezi z razkritjem občutljivih zdravstvenih podatkov tretjim osebam za namene trženja (https://www.ftc.gov/system/files/ftc_gov/pdf/MonumentOrderFiled.pdf).

[36] FTC je na primer nedavno napovedal preiskavo, ki je privedla do tožbe proti družbi TikTok in njeni matični družbi Bytedance zaradi domnevne kršitve zakona o zasebnosti otrok. Obe družbi domnevno nista izpolnili zahteve glede obveščanja in pridobitve soglasja staršev pred zbiranjem in uporabo osebnih podatkov otrok, mlajših od 13 let (https://www.ftc.gov/news-events/news/press-releases/2024/08/ftc-investigation-leads-lawsuit-against-tiktok-bytedance-flagrantly-violating-childrens-privacy-law).

[37] Glej pregled nedavnih dejavnosti izvrševanja v dokumentu FTC 2023 Privacy and Data Security Update (Najnovejše informacije FTC o zasebnosti in varnosti podatkov za leto 2023). https://ec.europa.eu/commission/presscorner/detail/en/mex_24_1307.

[38] Glej https://ec.europa.eu/commission/presscorner/detail/sl/mex_24_1307. Na podlagi seje marca 2024 je bilo sklenjeno, da bo organiziranih več tematskih sej. Prva je potekala julija 2024 in je bila osredotočena na razvoj orodij, ki lahko malim in srednjim podjetjem pomagajo pri spoštovanju zakonov o zasebnosti.

[39] Drugi ukrepi, ki jih je mogoče sprejeti v skladu s FISA v zvezi s podatki, prenesenimi iz EU, so individualizirani elektronski nadzor (člen 105 FISA), fizične preiskave (člen 302 FISA), uporaba snemalnikov klicev ali naprav za

ukrepov za obveščevalne dejavnosti SIGINT ZDA (v nadaljnjem besedilu: Odredba št. 14086), ki jo je predsednik ZDA sprejel 7. oktobra 2022. Zaščitni ukrepi iz Odredbe št. 14086 se uporabljajo za vse obveščevalne dejavnosti SIGINT v ZDA, ne glede na pravno podlago, na kateri temeljijo, in ne glede na to, kje potekajo, ter varujejo podatke nedržavljanov ZDA (vključno z Evropejci)[40]. Z Odredbo št. 14086 je bil vzpostavljen tudi nov mehanizem pravnih sredstev, prek katerega lahko posamezniki v EU uveljavljajo in izvršujejo te zaščitne ukrepe.

V naslednjih oddelkih so opisani ukrepi, ki so jih organi ZDA uvedli od sprejetja sklepa o ustreznosti za uskladitev z Odredbo št. 14086, ter razvoj dogodkov v zvezi z zgoraj navedenim pravnim okvirom.

2.2.1. Razvoj dogodkov v zvezi s pravnim okvirom ZDA

2.2.1.1. Izvajanje Odredbe št. 14086 s strani obveščevalnih agencij

Omejitve in zaščitni ukrepi, uvedeni z Odredbo št. 14086, dopolnjujejo omejitve in zaščitne ukrepe iz člena 702 FISA in Odredbe št. 12333. Zavezujoči so za vse obveščevalne agencije in so bili nadalje operacionalizirani s politikami in postopki, ki jih je sprejela posamezna agencija.

Organi ZDA so v okviru prvega pregleda potrdili, da Odredba št. 14086 od sprejetja ni bila spremenjena. Poleg tega je bilo pojasnjeno, da predsednik ZDA ni uporabil pooblastila iz člena 2(b)(i)(B) in 2(b)(ii)(C) Odredbe št. 14086 za posodobitev seznama zakonitih ciljev, za katere se lahko uporabljajo obveščevalni podatki v okviru SIGINT, ali seznama namenov, za katere se lahko uporabljajo množično zbrani podatki[41]. Za določitev bolj specifičnih obveščevalnih prednostnih nalog, za katere se lahko dejansko zbirajo obveščevalni podatki v okviru SIGINT, je bil z Odredbo št. 14086 vzpostavljen poseben postopek. Zlasti se je treba posvetovati z uradnico za varstvo zasebnosti in državljanskih svoboščin v okviru urada direktorja nacionalne obveščevalne službe (Civil Liberties Protection Officer of the Office of the Director of National Intelligence, v nadaljnjem besedilu: ODNI CLPO), da se za vsako prednostno nalogo oceni, ali (1) ta izboljšuje enega ali več zakonitih ciljev, določenih v Odredbi; (2) ni bila zasnovana za zbiranje obveščevalnih podatkov v okviru SIGINT za prepovedan cilj, določen v Odredbi, niti se ne predvideva, da bo povzročila tako zbiranje, in (3) je bila določena po ustreznem upoštevanju varstva zasebnosti in državljanskih svoboščin vseh ljudi[42]. ODNI CLPO je na pregledovalni seji potrdila, da je pregledala prednostne naloge, ki jih je direktor nacionalne obveščevalne službe (Director of National Intelligence, v nadaljnjem besedilu: DNI) predlagal v okviru nacionalnih obveščevalnih prednostnih nalog za leto 2023, ugotovila, da so v skladu z navedenimi zahtevami, in svoj sklep posredovala DNI, ki je nato prednostne naloge predložil v potrditev predsedniku. ODNI CLPO je zagotovila tudi usposabljanje o zahtevah iz Odredbe št. 14086 za dele obveščevalne skupnosti, ki sodelujejo pri oblikovanju obveščevalnih prednostnih nalog.

sledenje (člen 402 FISA) ter zbiranje poslovnih evidenc nekaterih družb (splošni prevozniki, ponudniki javnih objektov za nastanitev, objekti za izposojo vozil ali skladišča, člen 501 FISA). Te različne pravne podlage so podrobno analizirane v sklepu o ustreznosti (uvodne izjave 142–152).

[40] Za več informacij glej oddelek 3.2.1.2 sklepa o ustreznosti.

[41] Ti zakoniti cilji/nameni vključujejo na primer zaščito pred vohunjenjem, sabotažo, umori ali drugimi obveščevalnimi dejavnostmi, ki jih izvaja tuja vlada, organizacija ali oseba ali se izvajajo v njenem imenu ali s pomočjo tuje vlade, organizacije ali osebe; zaščito pred terorizmom, zajetjem talcev in zadrževanjem posameznikov v ujetništvu s strani ali v imenu tuje vlade, organizacije ali osebe.

[42] Člen 2(b)(iii) Odredbe št. 14086.

Organi ZDA so v preteklem letu tudi sprejeli nadaljnje praktične ukrepe za izvajanje Odredbe št. 14086 v svojih vsakodnevnih dejavnostih. Obveščevalne agencije so zlasti vzpostavile dodatne notranje politike in smernice o uporabi Odredbe, na primer notranje postopke (z zahtevami po notranji odobritvi, dokumentiranim nadzorom dostopa, tako da imajo dostop do informacij samo tisti posamezniki, ki so bili ustrezno usposobljeni in imajo potrebne zahteve glede nalog, itd.), da se zagotovi izpolnjevanje zahtev glede nujnosti in sorazmernosti v okviru ciljnega in množičnega zbiranja[43]. Poleg tega je bilo osebju različnih obveščevalnih agencij (npr. NSA, CIA, FBI) zagotovljeno usposabljanje o Odredbi št. 14086, vključno z letnimi in *ad hoc* usposabljanji, ki jih organizira ODNI CLPO, ter obveznimi usposabljanji za vse novo osebje, ki se pridruži ODNI.

Komisija pozdravlja različne ukrepe, sprejete za izvajanje Odredbe št. 14086 in zagotavljanje skladnosti z njo. Ko bo pridobljenih več izkušenj z uporabo zaščitnih ukrepov iz Odredbe v praksi, bi bila Komisija vesela priložnosti za razpravo o konkretnih primerih uporabe Odredbe v praksi (ob upoštevanju ustreznih pomislekov glede zaupnosti) v okviru prihodnjih pregledov.

2.2.1.2. Ponovna odobritev člena 702 FISA

Člen 702 FISA omogoča zbiranje tujih obveščevalnih podatkov s ciljnim osredotočanjem na nedržavljane ZDA, za katere se utemeljeno sklepa, da se nahajajo zunaj Združenih držav. Zbiranje poteka na podlagi letnih potrdil, ki se predložijo sodišču za nadzor nad tujo obveščevalno dejavnostjo (Foreign Intelligence Surveillance Court, v nadaljnjem besedilu: FISC) in ki jih to sodišče odobri. V potrdilih so opredeljene posebne kategorije tujih obveščevalnih podatkov, ki jih je treba zbrati. ODNI je 21. julija 2023 objavil, da obstajajo tri odobrena potrdila v skladu s členom 702 FISA, ki zajemajo naslednje kategorije tujih obveščevalnih podatkov: (1) tuje vlade in z njimi povezani subjekti, (2) boj proti terorizmu in (3) boj proti širjenju orožja[44]. Potrdila morajo vključevati tudi postopke izbire cilja in zmanjšanja, ki jih odobri FISC[45]. Izbira cilja se izvede zlasti tako, da se od ameriških družb, ki ustrezajo opredelitvi „ponudnika storitev elektronskih komunikacij“ iz FISA, zahteva, da razkrijejo elektronske komunikacijske podatke, poslane „izbirnikom“ ali prejete od njih, ki opredeljujejo poseben komunikacijski račun, npr. telefonsko številko ali e-poštni naslov. Vlada ZDA je objavila več gradiv o členu 702 FISA, da bi javnost obvestila o delovanju programov nadzora, veljavnih zahtevah in varstvu zasebnosti ter vlogi FISC[46].

Zaradi klavzule o časovni omejitvi veljavnosti naj bi člen 702 FISA prenehal veljati konec leta 2023, razen če ga kongres ponovno odobri. Po začasni ponovni odobritvi brez kakršnih koli sprememb je kongres 19. aprila 2024 sprejel zakon o reformi obveščevalnih služb in zagotavljanju varnosti Amerike (Reforming Intelligence and Securing America Act, v nadaljnjem besedilu: RISAA), s katerim je ponovno odobril člen 702 FISA za dve leti in uvedel več sprememb. Te spremembe je mogoče v grobem razdeliti v dve kategoriji: (1) spremembe obsega dejavnosti nadzora, dovoljenih v skladu s členom 702 FISA, ter (2) institucionalne in postopkovne spremembe.

---

[43] Glej https://www.intel.gov/ic-on-the-record-database/results/oversight/1278-odni-releases-ic-procedures-implementing-new-safeguardsin-executive-order-14086, objavljeno 3. julija 2023.

[44] https://www.intelligence.gov/ic-on-the-record-database/results/1307-release-of-documents-related-to-the-2023-fisa-section-702-certifications.

[45] Taki postopki omejujejo zbiranje podatkov v zvezi s posebnim namenom zbiranja tujih obveščevalnih podatkov, dostop do podatkovnih zbirk, v katerih so shranjene informacije, pridobljene na podlagi člena 702 FISA (vključno z nadzorom dostopa), ter uporabo, hrambo in razširjanje takih informacij.

[46] https://www.intel.gov/foreign-intelligence-surveillance-act.

Spremembe obsega dejavnosti nadzora, dovoljenih v skladu s členom 702 FISA

Z RISAA so bile uvedene tri glavne spremembe obsega nadzornih dejavnosti, ki se lahko izvajajo v skladu s členom 702 FISA.

Prvič, zbiranje informacij o ciljni osebi iz komunikacij med drugimi osebami je bilo dokončno prepovedano[47]. To se nanaša na zbiranje sporočil, pri katerih izbirnik iz člena 702 (kot je e-poštni naslov) ni v polju „za“ ali „od“ sporočil, temveč sporočila vsebujejo sklic na tak izbirnik (npr. elektronska sporočila, ki niso poslana na izbrani e-poštni naslov ali z njega, ampak vključujejo izbrani e-poštni naslov v besedilu ali vsebini elektronskega sporočila). Čeprav je bilo tako zbiranje podatkov izključeno že po spremembi FISA leta 2018, je bila v FISA še vedno predvidena možnost ponovnega začetka zbiranja informacij o ciljni osebi iz komunikacij med drugimi osebami v prihodnosti, in sicer po posebnem postopku odobritve, v katerega sta vključena FISC in kongres. Z zadnjo spremembo, uvedeno z RISAA, je bila ta možnost odpravljena.

Drugič, opredelitev tujih obveščevalnih podatkov je bila razširjena tako, da vključuje informacije v zvezi z bojem proti narkotikom[48]. Organi ZDA so na pregledovalni seji pojasnili, da so bili razlogi za to trenutna kriza s fentanilom in vse večje grožnje za nacionalno varnost, ki jo predstavljajo mednarodni preprodajalci in proizvajalci narkotikov. Glede na navedeno je bilo potrjeno, da ta pojem spada pod več zakonitih ciljev iz Odredbe št. 14086, tj. razumevanje ali ocenjevanje zmogljivosti, namenov ali dejavnosti tujih organizacij, ki predstavljajo sedanjo ali morebitno grožnjo za nacionalno varnost Združenih držav ali njenih zaveznikov, razumevanje ali ocenjevanje nadnacionalnih groženj, ki vplivajo na svetovno varnost, vključno s tveganji za javno zdravje, in zaščita pred nadnacionalnimi grožnjami kriminala[49].

Tretjič, z RISAA je bila razširjena opredelitev pojma „ponudnik storitev elektronskih komunikacij“, s čimer se je razširil obseg družb, ki so lahko zavezane zagotavljati informacije v skladu s členom 702 FISA[50]. Opredelitev zdaj vključuje „druge ponudnike storitev, ki imajo ‚dostop do opreme, ki se uporablja ali se lahko uporablja za prenos ali shranjevanje telefonskih ali elektronskih komunikacij‘“, pri čemer so izrecno izključeni javni objekti za nastanitev, stanovanja, javna infrastruktura in gostinski obrati. Ministrstvo za pravosodje se je v dopisu kongresu sklicevalo na to spremembo kot tehnično spremembo, ki naj bi zajela „izjemno majhno“ število tehnoloških družb, ki glede na nedavne odločbe FISC in pritožbenega sodišča za nadzor nad tujo obveščevalno dejavnostjo (Foreign Intelligence Surveillance Court of Review, v nadaljnjem besedilu: FISCR) niso bile zajete v prejšnji opredelitvi ponudnika storitev elektronskih komunikacij[51]. V istem dopisu se je ministrstvo za pravosodje zavezalo, da bo zožilo področje uporabe z uporabo te opredelitve izključno za vrsto ponudnika storitev, ki je predmet spora, na podlagi katerega je bila sprejeta odločba FISC. Zato so zadevne družbe navedene v tajni prilogi za kongres. Več nevladnih organizacij, vključno s tistimi, ki so v okviru pregleda predložile povratne informacije, je izrazilo pomisleke glede te razširitve z utemeljitvijo, da bi lahko zajela številne družbe v ZDA (saj mnoge od njih zagotavljajo neko

[47] Člen 22 RISAA.
[48] Člen 23 RISAA.
[49] Člen 2(b)(ii)(A)(2), (3) in (10) Odredbe št. 14086.
[50] Člen 25 RISAA.
[51] https://www.justice.gov/opa/media/1348621/dl?inline. Glej odločbo FISC iz leta 2022 (https://www.intel.gov/assets/documents/702%20Documents/declassified/2022-FISC-ECSP-OPINION.pdf) in sodbo pritožbenega sodišča za nadzor nad tujo obveščevalno dejavnostjo, s katero je bila ta odločba potrjena (https://www.intel.gov/assets/documents/702%20Documents/declassified/2023_FISC-R_ECSP_Opinion.pdf).

vrsto storitve in imajo dostop do komunikacijske opreme). Glede na te pomisleke je bila ob podpori obveščevalne skupnosti predlagana dodatna sprememba osnutka zakona o pooblastilih obveščevalnih služb za proračunsko leto 2025, ki je trenutno v obravnavi v kongresu. Če bi kongres to spremembo sprejel, bi bile dodatne družbe, zajete v opredelitvi ponudnika storitev elektronskih komunikacij, omejene le na tiste iz navedenih sodb FISC. Predlog zakona predvideva tudi, da bi bilo treba vsako direktivo, naslovljeno na tako družbo, sporočiti FISC, da bi ta lahko pregledal, ali bi družba dejansko spadala na področje uporabe. Ministrstvo za pravosodje se je v svojem pismu kongresu zavezalo, da mu bo vsakih šest mesecev poročalo o kakršni koli uporabi posodobljene opredelitve, da bi kongresu omogočilo izvajanje ustreznega nadzora v zvezi z ozko uporabo opredelitve.

Pomembno je, da so organi ZDA in PCLOB na pregledovalni seji potrdili, da se vsi zaščitni ukrepi iz Odredbe št. 14086 še naprej v celoti uporabljajo za vse zbiranje in uporabo podatkov na podlagi člena 702 FISA, tudi po teh spremembah. Čeprav se je z RISAA nekoliko razširil obseg družb, ki bi lahko pridobile odločbo, se uveljavljanje pravic zato ni omejilo. Kljub temu bo treba spremljati nadaljnji razvoj (zakonodajni in poročevalski) ter prejemati informacije o uporabi teh novih pravil v praksi. To vključuje na primer učinek širše opredelitve tujih obveščevalnih podatkov in ponudnikov storitev elektronskih komunikacij na število ciljnih oseb iz člena 702 FISA (kot jih vsako leto sporoči ODNI, glej spodaj v zvezi s preglednostjo). Prihodnje poročilo o nadaljnjih ukrepih na podlagi nedavnega poročila PCLOB o členu 702 FISA (glej spodaj) bi moralo biti v zvezi s tem posebno informativno.

Institucionalne in postopkovne spremembe

Kar zadeva institucionalne in postopkovne spremembe, je bilo z RISAA kodificiranih več postopkov, ki so se že izvajali v praksi, in uvedeni so bili novi zaščitni ukrepi. Medtem ko se nekatere od teh sprememb nanašajo le na državljane ZDA, več sprememb povečuje zaščito za državljane ZDA in za nedržavljane ZDA, katerih podatki se lahko zbirajo v skladu s členom 702 FISA[52], in so zato pomembne za delovanje DPF.

Prvič, uvedenih je bilo več dodatnih zahtev glede odgovornosti, nadzora in poročanja. Zlasti se mora osebje FBI zdaj vsako leto usposabljati o pravilih, ki se uporabljajo za poizvedovanje po informacijah, pridobljenih v skladu s členom 702 FISA[53]. FBI mora kongresu poročati tudi o svojih dejavnostih poizvedovanja (npr. o številu poizvedb z uporabo „tehnologij za paketna opravila“, tj. z uporabo več poizvedbenih izrazov v okviru ene poizvedbe) in o ukrepih glede odgovornosti, vzpostavljenih za zagotavljanje skladnosti s pravnimi zahtevami glede poizvedovanja (člena 11 in 12 RISAA). Poleg tega je generalnemu inšpektorju ministrstva za pravosodje naročeno, naj pripravi poročilo o skladnosti FBI z zahtevami glede poizvedovanja (člen 9 RISAA). Splošno gledano morata ODNI in generalni državni tožilec za povečanje preglednosti postopkov pred FISC pregled v zvezi z odpravo zaupnosti odločb FISC zdaj končati v 180 dneh (člen 7 RISAA). Poleg tega je treba hraniti prepise vseh obravnav pred

[52] Poleg tega so bile z RISAA uvedene nekatere spremembe v zvezi s tradicionalnim individualiziranim elektronskim nadzorom v skladu s členom 105 FISA (na podlagi naloga, ki ga FISC izda, če je izpolnjen standard utemeljenega suma). Obveščevalne agencije morajo vlogi, ki jo vložijo pri generalnem državnem tožilcu za odločbo o izvajanju individualiziranega elektronskega nadzora, zdaj priložiti zapriseženo izjavo, ki utemeljuje prepričanje, da so pogoji iz člena 105 FISA izpolnjeni (člen 6(a) RISAA). Morebitno trajanje elektronskega nadzora v zvezi s tujimi silami ali agenti tujih sil se je podaljšalo s 120 dni na eno leto (člen 6(g) RISAA).

[53] Člen 2(d) RISAA.

FISC in FISCR (kjer se je mogoče pritožiti zoper odločbe FISC) ter jih poslati kongresu (člen 8 RISAA).

Drugič, z RISAA so bile uvedene dodatne omejitve glede uporabe podatkov, zbranih na podlagi člena 702 FISA, s strani FBI. Člen 2(d) RISAA določa, da se poizvedba z uporabo „paketne tehnologije“ lahko opravi le na podlagi odobritve odvetnika pri FBI, razen v nujnih okoliščinah. Poleg tega FBI zdaj ne sme samodejno preverjati neminimiziranih informacij, pridobljenih v skladu s členom 702 FISA, temveč mora zagotoviti, da morajo analitiki potrditi izbiro iskanja po takih informacijah. Z RISAA FBI tudi ne sme izvajati poizvedb, ki so namenjene izključno iskanju in pridobivanju dokazov o kriminalni dejavnosti (razen če se utemeljeno domneva, da bi lahko pomagale ublažiti ali odpraviti grožnjo za življenje ali hudo telesno poškodbo, ali če je to potrebno za izpolnitev obveznosti razkritja v pravdnem postopku)[54]. FBI prav tako ne sme vnašati neminimiziranih podatkov v analitične repozitorije, razen če je ciljna oseba pomembna za obstoječo preiskavo nacionalne varnosti[55].

Tretjič, nekatere določbe v zvezi s statusom in vlogo *amici curiae* pred FISC so bile spremenjene[56]. *Amici* so določeni kot strokovnjaki, ki sodišču (in FISCR) pomagajo pri zadevah, povezanih z zasebnostjo in državljanskimi svoboščinami, ali pomagajo razjasniti tehnološka vprašanja pri obravnavi vloge določene vlade. Medtem ko so morali v skladu s FISA *amici* prej imeti strokovno znanje na področju zasebnosti in državljanskih svoboščin, zbiranja obveščevalnih podatkov, komunikacijske tehnologije ali drugih ustreznih področjih, morajo zdaj načeloma imeti strokovno znanje na področju zasebnosti / državljanskih svoboščin ter zbiranja obveščevalnih podatkov. Sodišče je že imelo možnost imenovati *amicus*, kadar koli se mu je to zdelo primerno, in je to moralo storiti pri obravnavi nove ali pomembne razlage prava. FISC mora po ponovni odobritvi zdaj imenovati *amicus* tudi vsakič, ko se ga zaprosi za odobritev potrdil na podlagi člena 702 FISA in spremljajočih postopkov (npr. postopkov izbire cilja), razen če ugotovi, da to ne bi bilo ustrezno ali bi verjetno povzročilo neupravičeno zamudo[57]. Poleg tega lahko sodišče zdaj imenuje enega ali več *amici*. Pojasnjeno je tudi, da morajo biti informacije, ki jih zagotovijo *amici* „omejene na obravnavo posebnih vprašanj, ki jih je ugotovilo sodišče“, čeprav so področja, o katerih lahko *amici* predložijo pripombe, še vedno široka (tj. pravni argumenti in informacije v zvezi z varstvom zasebnosti posameznikov in državljanskih svoboščin državljanov Združenih držav, zbiranje obveščevalnih podatkov in komunikacijska tehnologija ali katero koli drugo ustrezno področje).

Nazadnje, člen 18 RISAA vzpostavlja „komisijo za reformo FISA“, ki jo med drugim sestavljajo člani kongresa, predsednica PCLOB, glavni namestnik direktorja nacionalne obveščevalne službe in namestnik generalnega državnega tožilca ter dodatni člani, ki jih imenuje kongres[58], za priporočanje dodatnih reform FISA.

Komisija bo pozorno spremljala nadaljnji razvoj v zvezi s členom 702 FISA, tudi v okviru nadzornih dejavnosti PCLOB (glej v nadaljevanju), delo komisije za reformo in prihodnji pregled FISA po dveh letih.

---

[54] Člen 3(a) RISAA.

[55] Člen 3(b) RISAA. Kadar je to potrebno zaradi nujnih okoliščin, lahko direktor FBI odloči o izjemi od te določbe, o čemer je treba obvestiti kongres.

[56] Zaradi jasnosti te spremembe ne vplivajo na status in vlogo posebnih zagovornikov pred sodiščem za presojo varstva podatkov (Data Protection Review Court, v nadaljnjem besedilu: DPRC), kar so ZDA potrdile na pregledovalni seji.

[57] Člen 5(b) RISAA.

[58] Člen 18 izrecno zahteva, da predstavniki niso člani kongresa.

2.2.1.3. Dejavnosti nadzora v praksi: podatki in trendi

Letno statistično poročilo ODNI o preglednosti v zvezi z uporabo pristojnosti za nacionalni varnostni nadzor s strani obveščevalne skupnosti za koledarsko leto 2023 (objavljeno aprila 2024)[59] kaže, da se je število ciljnih oseb iz člena 702 FISA povečalo z 245 073 v koledarskem letu 2022 na 268 590 v koledarskem letu 2023. V poročilu je pojasnjeno, da so nihanja v številu ciljnih oseb lahko povezana z različnimi razlogi, vključno s spremembami operativnih prednostnih nalog, svetovnimi dogodki, tehničnimi zmogljivostmi, vedenjem ciljnih oseb in spremembami v telekomunikacijskem sektorju. V poročilu je navedeno tudi, da se na podlagi člena 402 FISA (snemalniki klicev ter naprave za sledenje) ni izvajal nadzor nad nobenim nedržavljanom ZDA (v primerjavi z enim leta 2021 in nič leta 2022), medtem ko je bilo na podlagi člena 501 FISA (dostop do poslovnih evidenc splošnih prevoznikov, ponudnikov javnih objektov za nastanitev, objektov za izposojo vozil ali skladišč) izdanih šest nalogov (v primerjavi z enajst leta 2021 in 2022) za šest ciljnih oseb (v primerjavi s 13 leta 2021 in 11 leta 2022), ki zajemajo 5 412 edinstvenih identifikatorjev (v primerjavi s 23 157 leta 2021 in 55 431 leta 2022), ki se uporabljajo za sporočanje informacij, zbranih na podlagi takih nalogov.

Ministrstvo za pravosodje je v letnem poročilu kongresu o zakonu o nadzoru tujih obveščevalnih podatkov navedlo, da je bilo v koledarskem letu 2023 pri FISC vloženih 327 vlog za izvajanje elektronskega nadzora in/ali fizičnih preiskav na podlagi člena 105 oziroma 302 FISA za namene tujih obveščevalnih podatkov[60]. Skupno število ciljnih oseb je bilo med 500 in 999. Glede sodnih pozivov v zvezi z nacionalno varnostjo (National Security Letter, v nadaljnjem besedilu: NSL) je v poročilu navedeno, da je bilo izdanih 10 115 zahtevkov za informacije o nedržavljanih ZDA (brez zahtevkov samo za informacije o naročnikih), da bi se pridobile informacije o 3 033 različnih nedržavljanih ZDA[61].

Več družb, certificiranih v okviru DPF (npr. Google, Meta), uporablja možnost, ki jo zagotavlja zakonodaja ZDA, za objavo poročil o preglednosti, ki vsebujejo informacije o številu zahtevkov FISA in NSL, prejetih v določenem obdobju poročanja. Med pripravo tega poročila statistični podatki o zahtevkih FISA po juliju 2023 še niso bili na voljo. Google je na primer poročal, da je med julijem in decembrom 2023 prejel od 500 do 999 zahtevkov na podlagi NSL, ki so se nanašali na 2 000 do 2 499 računov[62]. Družba Meta je poročala, da je v istem obdobju prejela od 0 do 499 zahtevkov na podlagi NSL, ki so se nanašali na 500 do 999 računov[63]. Številke se v zadnjih letih niso veliko spreminjale. Za dodatno povečanje preglednosti nekatere družbe (npr. Google) dejavno objavljajo NSL, ki so jih prejele, ko se odpravijo omejitve glede nerazkritja[64].

2.2.1.4. Drugi dogodki

[59] https://www.dni.gov/files/CLPT/documents/2024_ASTR_for_CY2023.pdf.
[60] https://www.justice.gov/nsd/media/1350236/dl?inline.
[61] Ti podatki so v primerjavi s prejšnjim letom poročanja (2022) ostali večinoma stabilni. Za primerjavo – leta 2022 je bilo pri FISC vloženih 317 končnih zahtevkov za elektronski nadzor in/ali fizične preiskave za namene tujih obveščevalnih podatkov. Skupno število oseb, na katere se nanašajo odločbe o elektronskem nadzoru, je znašalo med 0 in 499. FBI je leta 2022 vložil 9 103 zahtevkov na podlagi NSL za informacije o osebah, ki niso državljani ZDA (brez zahtevkov samo za informacije o naročnikih). Vir: https://irp.fas.org/agency/doj/fisa/2022rept.pdf.
[62] https://transparencyreport.google.com/user-data/us-national-security.
[63] https://transparency.meta.com/reports/government-data-requests/country/US/.
[64] https://transparencyreport.google.com/user-data/us-national-security..

V okviru priprave pregleda je več nevladnih organizacij zastavilo vprašanja o novih oblikah, ki jih obveščevalne agencije ZDA uporabljajo za pridobivanje podatkov z nakupom le-teh od komercialnih subjektov, zlasti posrednikov podatkov. Pojasnile so, da je treba podatke, zbrane na tej podlagi, sicer še vedno obdelovati v skladu z drugimi zahtevami, vključno na primer z Odredbo št. 12333[65], vendar se podatki pridobivajo zunaj okvira FISA in Odredbe št. 14086.

V zvezi s tem je treba opozoriti, da za vsako vrsto prostovoljne izmenjave podatkov s tretjimi osebami velja več podrobnih pogojev iz DPF. Prvič, certificirana organizacija si ne more izmenjevati podatkov s tretjo osebo (ki ne deluje kot posrednik/obdelovalec), ne da bi zadevne posameznike obvestila in jim omogočila izbiro[66]. Drugič, v skladu z *načelom odgovornosti za prenos tretjemu* se nadaljnji prenosi lahko izvedejo le (1) za omejene in določene namene, (2) na podlagi pogodbe med organizacijo v DPF EU-ZDA in tretjo osebo ter (3) samo, če navedena pogodba zagotavlja tretji stranki enako raven varstva, kot jo zagotavljajo načela[67].

Poleg tega je FTC, kot se je razpravljalo tudi na pregledovalni seji, sprejel izvršilne ukrepe proti posrednikom podatkov, ki prodajajo občutljive podatke o potrošnikih. Na primer, FTC je v zadevi proti družbi X-Mode in njeni družbi naslednici Outlogic 9. januarja 2024 sprejel odločbo, s katero je družbi prepovedal prodajo podatkov o geolokaciji tretjim osebam in naročil izbris podatkov, ki jih je nezakonito uporabljala in si jih izmenjevala. Preiskava FTC je med drugim pokazala, da družba posameznikov ni v celoti obvestila o uporabi in prodaji podatkov o njihovi geolokaciji, ni uvedla ukrepov, ki bi posameznikom omogočali, da zavrnejo sledenje, dovolila je uporabo podatkov za potencialno diskriminatorne namene in ni omejila uporabe takih informacij pri tretjih osebah[68]. Komisija pričakuje, da bo FTC sprejel enak pristop, če bi si družbe, certificirane v okviru DPF, izmenjavale podatke v nasprotju z zgoraj navedenimi določbami.

Nazadnje je treba omeniti, da je ODNI maja 2024 izdal okvir politike obveščevalne skupnosti za komercialno dostopne informacije[69]. Ta okvir določa številna načela in zahteve, ki bi jih morale obveščevalne agencije upoštevati pri pridobivanju in uporabi informacij v okviru trgovinskega posla, da bi se med drugim zmanjšala tveganja za zasebnost in državljanske svoboščine.

2.2.2. Neodvisen nadzor

Dejavnosti ameriških obveščevalnih agencij nadzorujejo različni organi, med drugim uradniki za varstvo zasebnosti in državljanskih svoboščin, generalni inšpektorji, kongres in PCLOB. Odredba št. 14086 zlasti zahteva, da ima vsaka obveščevalna agencija višje uradnike za pravne zadeve, nadzor in skladnost, da se zagotovi skladnost z zakonodajo ZDA, ki se uporablja. To nadzorno funkcijo uradniki izpolnjujejo v vlogi imenovanih presojevalcev skladnosti, pa tudi

[65] Glej na primer člen 2.4 Odredbe št. 12333 o tehnikah zbiranja.
[66] Glej uvodno izjavo 40 sklepa o ustreznosti.
[67] Glej uvodno izjavo 38 sklepa o ustreznosti.
[68] https://www.ftc.gov/news-events/news/press-releases/2024/01/ftc-order-prohibits-data-broker-x-mode-social-outlogic-selling-sensitive-location-data.
[69] https://www.dni.gov/files/ODNI/documents/CAI/Commercially-Available-Information-Framework-May2024.pdf. Obveščevalne agencije morajo okvir spoštovati od avgusta 2024.

kot uradniki za varstvo zasebnosti in državljanskih svoboščin ter generalni inšpektorji[70]. Izvajati morajo reden nadzor nad obveščevalnimi dejavnostmi SIGINT in zagotavljati odpravo vsake neskladnosti. Obveščevalne agencije morajo takim uradnikom za izvajanje njihovih nadzornih funkcij zagotoviti dostop do vseh ustreznih informacij in ne smejo sprejeti nobenih ukrepov, s katerimi bi ovirale ali neustrezno vplivale na njihove dejavnosti nadzora.

Na pregledovalni seji je sodeloval glavni svetovalec urada generalnega inšpektorja obveščevalne skupnosti (Office of the Intelligence Community Inspector General, v nadaljnjem besedilu: ICIG) v ODNI – ki ima celovito pristojnost nad celotno obveščevalno skupnostjo in je pooblaščen za preiskovanje pritožb ali informacij v zvezi z domnevnim nezakonitim ravnanjem ali zlorabo pooblastil. Potrdil je, da ICIG v okviru svojih dejavnosti nadzora sistematično preverja skladnost z Odredbo št. 14086. Omenil je tudi nedavne dejavnosti nadzora drugih generalnih inšpektorjev obveščevalne skupnosti, kot je podrobno opisano v rednih poročilih. Na primer, v polletnem poročilu kongresu za obdobje od aprila do septembra 2023[71] je generalni inšpektor agencije za nacionalno varnost (National Security Agency, v nadaljnjem besedilu: NSA) sporočil oceno okvira notranje kontrole NSA za odločitve in zahteve o izbiri cilja. Ugotovil je, da okvir deluje pravilno in zagotavlja skladnost z zakoni, direktivami in politikami, ki varujejo državljanske svoboščine in zasebnost. V istem poročilu je omenjena tudi preiskava, ki je razkrila zlorabo obveščevalnega orodja SIGINT za nepooblaščene namene s strani uslužbenca NSA.

PCLOB ima v skladu z Odredbo št. 14086[72] posebne nadzorne funkcije[73]. Predsednica in vsi trije člani PCLOB so se udeležili pregledovalne seje in sporočili, da je PCLOB aprila 2023 obveščevalnim agencijam svetoval o njihovih osnutkih politik in postopkov za izvajanje Odredbe št. 14086 ter da je bilo z njim opravljeno posvetovanje o imenovanju sodnikov DPRC in posebnih pravobranilcev. Odbor je začel tudi projekt nadzora za (1) pregled izvajanja posodobljenih politik in postopkov, ki so jih sprejele obveščevalne agencije, da bi zagotovile njihovo skladnost z Odredbo, in (2) izvedbo letnega pregleda delovanja novega mehanizma pravnih sredstev (glej v nadaljevanju)[74]. Člani PCLOB so potrdili, da namerava odbor oba pregleda izvesti v bližnji prihodnosti. V zvezi s pravnimi sredstvi so pojasnili, da bo pregled PCLOB, če ne bo pritožb, osredotočen na politike in postopke, uvedene za vzpostavitev mehanizma.

---

[70] Vsaka obveščevalna agencija ima generalnega inšpektorja, ki je zakonsko neodvisen in pristojen za izvajanje revizij in preiskav v zvezi z dejavnostmi, ki jih izvaja zadevna agencija za namene nacionalne varnosti. Imajo dostop do vsega ustreznega (tudi tajnega) gradiva, po potrebi s sodnim pozivom, in lahko opravljajo zaslišanja. Generalni inšpektorji odstopijo zadeve suma kršitev kazenskega prava organom pregona, vodjem agencij pa izdajajo priporočila za popravne ukrepe. Čeprav njihova priporočila niso zavezujoča, so njihova poročila, vključno s poročili o nadaljnjih ukrepih (ali odsotnosti ukrepov), na splošno objavljena in se pošljejo kongresu. V zvezi s tem glej opombo 136 sklepa o ustreznosti glede vloge generalnega inšpektorja.

[71] https://oig.nsa.gov/reports/Article/3609957/semiannual-report-to-congress-1-april-2023-to-30-september-2023/.

[72] PCLOB je neodvisna agencija s pooblastili na področju politik boja proti terorizmu in njihovega izvajanja z namenom varstva zasebnosti in državljanskih svoboščin. Dostopa lahko do vseh ustreznih (tudi zaupnih) informacij, opravlja pogovore in prisostvuje zaslišanjem. Lahko izdaja priporočila organom kazenskega pregona in obveščevalnim organom ter redno poroča kongresu in predsedniku. Njena poročila so čim bolj javno dostopna.

[73] https://documents.pclob.gov/prod/Documents/EventsAndPress/834a1977-f420-4b2a-ae93-8a522b2c7c74/Trans-Atlantic%20Data%20Privacy%20Framework%20EO%20press%20release%20(FINAL)%20-%20Completed%20508%20-%2010202022.pdf.

[74] https://www.pclob.gov/OversightProjects/Details/1115.

Kar zadeva druge dejavnosti nadzora, je PCLOB 28. septembra 2023 izdal poročilo o členu 702 FISA[75]. To poročilo je nadaljevanje prejšnjega poročila iz leta 2014 ter vsebuje posodobljene dejanske in pravne informacije o delovanju programov nadzora iz člena 702 FISA. Poročilo vsebuje tudi priporočila o skladnosti obveščevalnih agencij z veljavnimi zahtevami in predloge kongresu za nadaljnjo krepitev več vidikov člena 702 FISA v okviru njegove ponovne odobritve (vključno s kodifikacijo zakonitih ciljev za dejavnosti nadzora iz Odredbe št. 14086)[76]. PCLOB je na pregledovalni seji sporočil, da pričakuje, da bo kmalu prejel odgovore obveščevalnih agencij o izvajanju njegovih priporočil, ki se bodo upoštevali v prihodnjem poročilu o nadaljnjih ukrepih. Drugi tekoči projekti nadzora vključujejo projekt o boju proti domačemu terorizmu in njegovemu vplivu na zasebnost in državljanske svoboščine ter zbiranje odprtokodnih ali komercialno dostopnih podatkov, ki ga izvaja FBI[77].

Nazadnje, nevladne organizacije, s katerimi so potekala posvetovanja v okviru pregleda, so izrazile zaskrbljenost glede izteka mandata več članov PCLOB v bližnji prihodnosti, zaradi česar bi lahko PCLOB postal nesklepčen. Mandat predsednice se je iztekel in obdobje predaje funkcije se konča januarja 2025, medtem ko je drugo delovno mesto prosto, tretje pa se bo prav tako sprostilo januarja naslednje leto. Člani so na pregledovalni seji pojasnili, da ne pričakujejo, da bo PCLOB na koncu nesklepčen, saj je bil za delovno mesto, ki je trenutno nezasedeno, že predlagan kandidat (ki čaka na potrditev senata)[78]. Poudarili so še, da tudi če bi odbor postal nesklepčen, to ne bi vplivalo na njegovo zmožnost nadaljnjega izvajanja projektov nadzora. Kljub temu bo Komisija glede na pomembno vlogo PCLOB pri pregledu izvajanja Odredbe št. 14086 pozorno spremljala status prihodnjih prostih delovnih mest in predlaganj/imenovanj.

2.2.3. Pravna sredstva

Na podlagi Odredbe št. 14086, dopolnjene z uredbo pravosodnega ministra, je vzpostavljen nov mehanizem pravnih sredstev za obravnavanje in reševanje upravičenih pritožb posameznikov, ki se nanašajo na ameriške obveščevalne dejavnosti SIGINT[79]. Vsak posameznik v EU ima pravico mehanizmu pravnih sredstev predložiti pritožbo, ki se nanaša na domnevno kršitev ameriškega zakona, ki ureja obveščevalne dejavnosti SIGINT (npr. Odredba št. 14086, člen 702 FISA, Odredba št. 12333), in negativno vpliva na njegove interese glede varstva zasebnosti in državljanskih svoboščin. Posamezniki lahko vložijo pritožbo pri organu za varstvo podatkov v državi članici EU, ki prek sekretariata EOVP pritožbo posreduje v mehanizem pravnih sredstev. Mehanizem je sestavljen iz dveh plasti, in sicer prvotne preiskave pritožb, ki jo izvaja ODNI CLPO, in možnosti posameznikov, da vložijo pritožbo zoper odločbo CLPO pred neodvisnim DPRC. Ko ODNI CLPO ali DPRC zaključi pregled, nacionalni organ posameznike obvesti, da „pri pregledu bodisi niso bile ugotovljene nobene zajete kršitve bodisi je ODNI CLPO/DPRC izdal odločitev, ki zahteva ustrezno odpravo kršitve“. Odločbe ODNI CLPO in DPRC so za obveščevalne agencije zavezujoče.

---

[75] https://documents.pclob.gov/prod/Documents/OversightReport/8ca320e5-01d3-4d6a-8106-3384aad6ff31/2023%20PCLOB%20702%20Report%20-%20Nov%2017%202023%20-%201446.pdf.

[76] Komisija ugotavlja, da so bila nekatera od teh priporočil vključena kot del RISAA, vključno s priporočilom o zbiranju informacij o ciljni osebi iz komunikacij med drugimi osebami ali priporočilom o krepitvi vloge strokovnjakov FISC (*amici*).

[77] https://www.pclob.gov/OversightProjects.

[78] https://documents.pclob.gov/prod/Documents/EventsAndPress/deb9cd13-12af-4250-998e-a520a2419a6b/PCLOB%20nominee%20press%20release%206-13-24.pdf.

[79] Uvodne izjave 176–194 sklepa o ustreznosti.

Od sprejetja sklepa o ustreznosti so bili sprejeti nadaljnji ukrepi, da bi mehanizem pravnih sredstev postal v celoti delujoč.

Kar zadeva ustanovitev DPRC, je bilo 14. novembra 2023 na sodišče imenovanih osem sodnikov (tj. dva več kot je najmanjše število na podlagi Odredbe št. 14086, kakor je bila dopolnjena z uredbo pravosodnega ministra v poglavju 28, člen 201.3(a), zveznega zakonika Združenih držav Amerike)[80]. Imenovani so bili na podlagi meril iz Odredbe št. 14086 in v skladu s postopkom, določenim v navedeni odredbi, med drugim tudi po posvetovanju s PCLOB[81]. Med njimi so nekdanji sodniki zveznega okrožnega sodišča in pritožbenega sodišča, nekdanji generalni državni tožilec ZDA in nekdanji član PCLOB. V skladu z navedeno odredbo ima vsaj polovica sodnikov predhodne sodniške izkušnje. Poleg tega sta bila aprila 2024 imenovana dva posebna pravobranilca, in sicer delavca v pravni stroki s strokovnim znanjem na področju zasebnosti in nacionalne varnosti, ki zastopata interese posameznikov pred DPRC. Na pregledovalni seji je bilo potrjeno, da so vsi sodniki in posebni pravobranilci prejeli najvišje varnostno potrdilo in imajo lahko zato pri opravljanju svojih nalog za DPRC dostop do tajnega gradiva. DPRC je objavil tudi vrsto pogosto zastavljenih vprašanj z informacijami o svoji vlogi, neodvisnosti in delovanju[82].

Kar zadeva obravnavo pritožb, je ODNI 6. decembra 2022 sprejel direktivo o obveščevalni skupnosti št. 126, ki podrobno ureja različne vidike postopka preiskave in odločanja o pritožbah (z določitvijo rokov, vzpostavitvijo varnega elektronskega repozitorija in komunikacijskih kanalov, zahtevo, da CLPO in obveščevalne skupnosti sodelujejo s PCLOB v okviru letnega pregleda mehanizma pravnih sredstev, itd.)[83]. Direktiva se uporablja v celotni obveščevalni skupnosti ZDA in je bila dopolnjena z nadaljnjimi notranjimi postopki, ki so jih posamezne obveščevalne agencije sprejele v zvezi s sodelovanjem z ODNI CLPO v okviru obravnavanja pritožb (npr. razvoj varnega repozitorija za izmenjavo pritožb in zadevnih dokumentov ter varno komuniciranje med ustreznimi agencijami). DPRC bo v prihodnjih mesecih izdal tudi podrobnejša pravila o obravnavanju pritožb in drugih postopkovnih vidikih.

V Evropski uniji in Združenih državah so bili sprejeti številni dodatni ukrepi za obveščanje širše javnosti ter olajšanje predložitve in obravnave pritožb. To vključuje sprejetje informativnega dokumenta o novem mehanizmu pravnih sredstev[84] s strani EOVP, predlogo obrazca za pritožbe (ki naj bi jo vsi organi za varstvo podatkov prevedli in objavili v svojih nacionalnih jezikih)[85] in poslovnik, ki ureja sodelovanje med nacionalnimi nadzornimi organi in sekretariatom EOVP[86]. Podobno je ODNI objavil pogosto zastavljena vprašanja in

[80] https://www.justice.gov/opa/pr/attorney-general-merrick-b-garland-announces-judges-data-protection-review-court.
[81] Člen 3(d)(A) Odredbe št. 14086.
[82] https://www.justice.gov/opcl/dprc-resources.
[83] https://www.dni.gov/files/documents/ICD/ICD_126-Implementation-Procedures-for-SIGINT-Redress-Mechanism.pdf.
[84] https://www.edpb.europa.eu/our-work-tools/our-documents/other-guidance/information-note-data-protection-framework-redress_sl.
[85] https://www.edpb.europa.eu/our-work-tools/our-documents/other-guidance/template-complaint-form-us-office-director-national_sl.
[86] https://www.edpb.europa.eu/our-work-tools/our-documents/other-guidance/rules-procedure-data-protection-framework-redress_sl.

informativni pregled o novem mehanizmu pravnih sredstev ter sodeloval pri dejavnostih ozaveščanja javnosti[87].

Poleg tega so EOVP in ustrezni organi ZDA v preteklem letu tesno sodelovali pri več operativnih vidikih. Kot je bilo potrjeno na pregledovalni seji, so zlasti vzpostavili šifriran komunikacijski kanal za posredovanje pritožb nacionalnih organov v EU sekretariatu EOVP, od sekretariata EOVP do ODNI CLPO in urada ministrstva za pravosodje za varstvo zasebnosti in državljanskih svoboščin (Office of Privacy and Civil Liberties, v nadaljnjem besedilu: OPCL) ter med ODNI CLPO in drugimi organi na strani ZDA (npr. DPRC). ODNI CLPO je pojasnila tudi, da so bili vzpostavljeni nadaljnji notranji postopki za sodelovanje posameznih obveščevalnih agencij z ODNI CLPO v zvezi z obravnavo pritožb.

OPCL, ki zagotavlja upravno podporo DPRC, je še sporočil, da DPRC deluje v okviru svoje posebne proračunske vrstice in ima potrebne zmogljivosti za izvajanje svojih nalog, vključno z varnimi računalniki in prenosnimi računalniki, telefoni itd. Poleg tega je ministrstvo za trgovino v skladu z Odredbo št. 14086 sprejelo potrebne ukrepe za vodenje evidence vseh prejetih upravičenih pritožb, vključno z vzpostavitvijo šifriranega komunikacijskega kanala z ODNI CLPO. Ministrstvo za trgovino bo pri ODNI CLPO redno poizvedovalo, ali je bila stopnja tajnosti informacij v zvezi s posamezno pritožbo preklicana. V tem primeru ministrstvo za trgovino o tem obvesti zadevnega posameznika, da mu omogoči dostop do takih informacij.

Nadzorni organi EU med pregledovalno sejo niso prejeli nobenih pritožb, zato novi mehanizem pravnih sredstev še ni bil sprožen.

3. ZAKLJUČEK

Komisija na podlagi informacij, zbranih med prvim pregledom, ugotavlja, da so organi ZDA vzpostavili potrebne strukture in postopke za zagotovitev učinkovitega delovanja okvira za varstvo zasebnosti podatkov. V zvezi s tem Komisija zelo ceni odlično sodelovanje z organi ZDA pri izvajanju pregleda.

Medtem ko je bil prvi pregled seveda osredotočen na preverjanje, ali so vzpostavljeni vsi sestavni elementi okvira, so izkušnje s praktično uporabo zaščitnih ukrepov, ki jih certificirane družbe uporabljajo za obdelavo podatkov in javni organi za dostop do podatkov, po samo enem letu delovanja vsekakor omejene. Komisija bo zato v naslednjih mesecih in letih pozorno spremljala razvoj dogodkov na zadevnem področju, pri čemer bo posebno pozornost namenila (1) prihodnjim poročilom PCLOB o izvajanju Odredbe št. 14086 in delovanju mehanizma pravnih sredstev SIGINT, zlasti DPRC; (2) morebitnim dodatnim spremembam člena 702 FISA ter (3) predlaganju in imenovanju članov PCLOB za zapolnitev prihodnjih prostih delovnih mest.

Poleg tega Komisija za zagotovitev stalnega in učinkovitega delovanja meni, da je pomembno, da:

[87] https://www.dni.gov/files/CLPT/documents/Fact_Sheets/The_Role_of_the_ODNI_CLPO_FAQs.pdf in https://www.dni.gov/files/CLPT/documents/Fact_Sheets/Data_Privacy_Framework.pdf.

— kot je bilo napovedano na pregledovalni seji, ministrstvo za trgovino bolje izkoristi različna orodja iz DPF za spremljanje skladnosti družb z načeli in odkrivanje lažnih navedb o sodelovanju,

— FTC še naprej razvija dejaven pristop k preiskovanju in uveljavljanju skladnosti certificiranih družb z načeli DPF ter

— ministrstvo za trgovino, FTC in organi EU za varstvo podatkov bi razvijejo skupne instrumente s smernicami o ključnih zahtevah v skladu z načeli DPF, npr. o podatkih o človeških virih in nadaljnjih prenosih.

Glede na ta rezultat pregleda in kot je predvideno v uvodni izjavi 211 sklepa o ustreznosti, Komisija meni, da bi bilo naslednji redni pregled primerno izvesti po treh letih. To bi moralo omogočiti, da se pridobi več izkušenj z uporabo DPF v praksi in upošteva navedeni prihodnji razvoj dogodkov. Komisija se bo zato v skladu s členom 3(4) sklepa o ustreznosti o pogostosti nadaljnjih pregledov posvetovala z EOVP in odborom, ustanovljenim v skladu s členom 93(1) splošne uredbe o varstvu podatkov.